

## UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

FILED

NOV 6 2018

Mark C. McCartt, Clerk  
U.S. DISTRICT COURT

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Samsung Galaxy, Mod. SM-J327AZ, SN:  
R28J81A2L6T (unknown number) 2) Samsung, Mod. SMJ120AZ,  
SN: R58J60FEMNE (unknown phone number) 3) Samsung, Mod. SM-  
G900A, SN: R38F50M7TVE (unknown phone number) 4) Samsung  
Galaxy S8, Mod. SM-G950U, SN: R38J90PTQVT, 405-437-9940 5)  
LG, Mod. LG-440G, SN: 01416200383733504, 918-934-0224 6)  
Alcatel, Mod. 4044C, IMEI:014896000500848, (unknown phone  
number) 7) LG, Mod. M257LG, SN: 801CYEA357652, 918-442-  
5955

Case No.

18-mj-147-PJC

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A":

located in the Northern District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B" and Attachment "C"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

21 U.S.C. § 846

21 U.S.C. § 841(a)(1)

21 U.S.C. § 844

Conspiracy

Possession with Intent to Distribute and Distribution of Marijuana

Possession of a Controlled Substance

The application is based on these facts:

See Affidavit of SA Holley J. Edwards, ATF attached hereto.

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more \_\_\_\_\_) is requested  
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

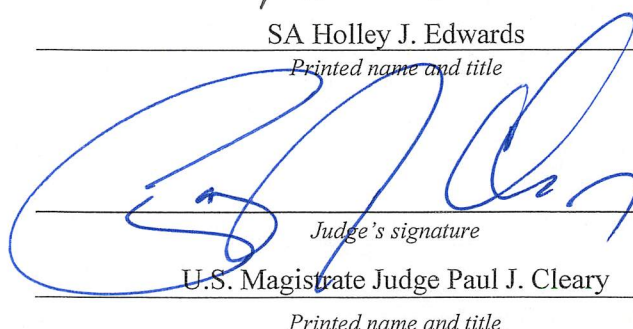
SA Holley J. Edwards  
Printed name and title

i

Sworn to before me and signed in my presence.

Date: 11/6/2018

City and state: Tulsa, OK

  
Judge's signature  
U.S. Magistrate Judge Paul J. Cleary  
Printed name and title

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Holley J. Edwards, having been duly sworn, do depose and state as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices (Attachment A)—which are currently in law enforcement possession, and the extraction from that property of electronically-stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and have been since September 2005. I am currently assigned to the Tulsa, Oklahoma Field Office. During my tenure as a Special Agent, I have participated in numerous investigations regarding narcotics trafficking, money laundering, violent crimes, firearms trafficking, convicted felons in possession of firearms, and the illegal use of firearms as it pertains to those prohibited from possessing firearms. As such, I have conducted physical surveillance operations, participated and been the Affiant on several search warrants, and participated in debriefings of confidential informants/sources. I have investigated violations of federal firearms and narcotics laws as they relate to the illegal use of firearms and narcotics in the commission of crimes.

3. Additionally, I have received training and conducted investigations involving organized criminal gangs and drug trafficking organizations. I have participated in physical surveillance, surveillance of undercover transactions, the execution of search warrants, examination of cellular phones, debriefings of informants, and I have conducted interviews of individuals involved in drug trafficking, viewed short message service (SMS) text messages involving the sale of firearms and drugs, and participated in undercover hand-to-hand buys both as a member of a

surveillance team and as an undercover agent. I have consulted with other law enforcement officers and agents about the trafficking and sale of firearms and drugs.

### **BACKGROUND INFORMATION**

4. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the actual cellular telephone. This data and information is oftentimes also maintained by the various service providers on separate equipment.

5. Based on my training, education, and experience, I have become familiar with the manner in which drug traffickers coordinate illegal activity, conduct illegal activity, and the communication methods used to conduct illegal activity. I have learned the following:

- a. Drug distributors/traffickers commonly maintain books, records, receipts, notes, ledgers, and other documents/papers both electronically and in paper form, which relate to the transportation, ordering, sale, and distribution of controlled substances, even though such documents may be in code and/or identify customers/sources/co-conspirators through monikers/nicknames. Documentation such as this oftentimes results because drug distributors/traffickers commonly “front” drugs (provide controlled substances on consignment) to their clients and must account for these transactions in order to collect outstanding drug debts.
- b. Drug distributors/traffickers commonly maintain addresses or telephone numbers in notebooks, papers, cellular phones, computers and electronic storage media which reflect names, address, and/or telephone numbers for their associates in the drug distribution/trafficking organization, even if said items may be in code, and such traffickers send and receive items listed in this affidavit by mail and other common carriers.
- c. Drug users, distributors and traffickers frequently take, or cause to be taken photographs or videotapes of themselves, their associates, their property/assets,

and their product, and these individuals usually maintain these photographs or recordings/videos in the residences under their control. These photographs and videos are also often found in the individual's cellular telephone, computers and other electronic storage media.

- d. I have participated in numerous searches of cellular telephones found to be in the possession of drug users/dealers/traffickers where text messages were discovered discussing topics such as quantities, prices and the quality of controlled dangerous substances, as well as dates, times and locations for drug transactions are discussed. Almost always, these communications are in coded drug talk/jargon and require review by peace officers experienced in deciphering such communications.
- e. In my experience in searching cellular telephones possessed by known drug users/distributors/traffickers, photos and/or videos have been discovered which evidence the use and distribution of controlled dangerous substances and the proceeds intended for or derived therefrom. Commonly said evidence depicts pictures/videos of drugs for evidencing the respective drugs quality, condition or quantity. Moreover, users will commonly document episodes of drug use in social settings. Additionally, drug distributors will take pictures ("trophy" pictures) or otherwise capture digital recordings for the purpose of memorializing their credibility/capability as a drug dealer and accomplishments (acquisition of assets/large amounts of U.S. currency) relating thereto.
- f. In all phases of drug distribution, the utilization of cellular telephones is essential. Drug users/dealers/traffickers use cellular telephones to place calls, as well as communicate by SMS text messaging. As drug dealing necessarily entails constant communications with accomplices, co-conspirators, clients, and sources, these communications virtually always take place by voice calls and text messaging over cellular telephones.
- g. Cellular telephones are almost always used by drug distributors as a way to communicate. They will communicate by verbal conversations, digital text messaging, and/or sending photographs to one another. To avoid detection, drug distributors will often times speak in coded language or through use of vague messages. Sometimes the cellular telephone numbers they use are listed in different individuals' name or they will frequently change phone numbers. Drug distributors will often "drop" or switch cellular phones to avoid detection by law enforcement. This will result in the accumulation of several different cellular phones.

6. As such, Affiant is seeking court authority to search individual cell phones described herein as well as court orders directing specific service providers to provide additional information and potentially stored wired and electronic information. This affidavit is made in support of requests to the court for warrants and/or orders to inspect, review and retrieve various information including but not limited to cell tower information, records, stored wired and electronic communications, photographic images and other information more further described herein relating to cellular telephones believed to have been used in the commission of various federal offenses.

7. The request for issuance of a search warrant is made for the seizure of physical evidence of the above-referenced offenses, any and all information and or data stored in the referenced cellular telephones, to include but not be limited to: the telephone number of the referenced cellular telephone(s), direct connect push-to-talk number of the referenced cellular telephone(s), telephone numbers calling the referenced telephone(s), calls made, received and missed, telephone numbers called by the referenced telephone(s), address and phone books stored within the referenced cellular telephone(s), and any text messages sent, received, saved and found in the referenced telephone(s), voice mails made, received, and saved, calendars, stored photos and digital records, web site visits history, as well as all other stored electronic data and information. (See Attachment A).

8. Service providers maintain additional information including electronic records that detail the "cell towers" or "cell sites" accessed by the aforementioned cellular telephones when the devices were used to receive calls, make calls, send text messages, etc. This information will provide data and evidence of the physical movement of the devices and/or their

users.

9. Information contained in this Affidavit is based upon my personal knowledge and also from discussions I have had with other law enforcement officers who have investigated these offenses.

### **CASE BACKGROUND**

10. On January 4, 2018, United States Probation (USP) Officer Bethany Blackmon went to the residence of Seth BRUSS, 5123 W. 8<sup>th</sup> Street, Tulsa, Oklahoma 74137, in order to conduct a home check pursuant to the terms of BRUSS' Federal Supervised Release. While inside BRUSS' residence, USP Officer Blackmon observed a plastic baggie with marijuana on the bathroom counter. The marijuana was confiscated by USP Officer Blackmon.

11. On April 20, 2018, the USP conducted a search of BRUSS' residence pursuant to the search conditions of BRUSS' Supervised Release. During the search, USP Officer's located marijuana in the kitchen and a bedroom. USP Officer Blackmon also seized seven cellular phones from BRUSS' residence. One cell phone, a Samsung Galaxy S8, located on the kitchen counter, contained photographs of large quantities of marijuana and money that were on BRUSS' dining room table, as well as a photograph of a large quantity of marijuana and what appears to be a scale commonly used to weigh narcotics, on BRUSS' kitchen counter (see Attachment C).

12. The cellular phones recovered from 5123 W. 8<sup>th</sup> Street were taken into custody by the United States Probation Office Northern District of Oklahoma.

### **CELLULAR TELEPHONES**

13. During a search of the above described residence, seven (7) cellular telephones were found within the residence. The aforementioned cellular telephones are currently located at

333 W. 4<sup>th</sup> Street, Suite 3820, Tulsa, Oklahoma. They are identified as:

- 1) Samsung Galaxy, Mod. SM-J327AZ, SN: R28J81A2L6T (unknown number)
- 2) Samsung, Mod. SMJ120AZ, SN: R58J60FEMNE (unknown phone number)
- 3) Samsung, Mod. SM-G900A, SN: R38F50M7TVE (unknown phone number)
- 4) Samsung Galaxy S8, Mod. Sm-G95OU, SN: R38J90PTQVT, 405-437-9940
- 5) LG, Mod. LG-440G, SN: 01416200383733504, 918-934-0224
- 6) Alcatel, Mod. 4044C, IMEI: 014896000500848, (unknown phone number)
- 7) LG, Mod. M257LG, SN: 801CYEA357652, 918-442-5855

14. The applied-for warrant would authorize the forensic examination of the aforementioned devices for the purpose of identifying electronically-stored data particularly described in Attachment B.

15. Based on the above information, Affiant believes there is probable cause that the phones described herein were used by BRUSS to communicate and facilitate the commission of drug trafficking activity, in violation of Title 21, United States Code, Section 846 (Conspiracy); Title 21, United States Code, Section 841(a)(1) (Possession with intent to distribute and distribution of marijuana), and Title 21, United States Code, Section 844 (Possession of a controlled substance). Affiant therefore respectfully requests a warrant and/or the appropriate Orders be issued for the search of cellular phones and phone records associated with the above referenced phones and phone numbers.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet

are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. There is probable cause to believe that things that were once stored on the devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that smartphone files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a smartphone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the smartphone may retain a log or record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, electronic storage media may contain electronic evidence of how a device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically-stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were

used, the purpose of their use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Device file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically-stored information on a storage medium is a dynamic process. Whether data stored on a device is evidence may depend on other information stored on the computer and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is, or is not, present on a storage medium.
- f. I know that when an individual uses an electronic device as a communication device or a device to obtain information from the Internet related to a criminal act, the individual’s electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime.

From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Further Affiant sayeth not.

  
ATF Special Agent  
Holley J. Edwards

SWORN to before me on November 6, 2018.

  
PAUL J. CLEARY  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

The property to be searched are seven (7) cellular phones:

1) Samsung Galaxy, Mod. SM-J327AZ, SN: R28J81A2L6T (unknown number),

IMEI: 355602080964665

2) Samsung, Mod. SMJ120AZ, SN: R58J60FEMNE (unknown phone number),

IMEI: 356903086071722

3) Samsung, Mod. SM-G900A, SN: R38F50M7TVE (unknown phone number),

IMEI: 353920061039691

4) Samsung Galaxy S8, Mod. Sm-G95OU, SN: R38J90PTQVT, 405-437-9940,

IMEI: 357066080581598

5) LG, Mod. LG-440G, SN: 01416200383733504, 918-934-0224, TracFone

Wireless

6) Alcatel, Mod. 4044C, IMEI: 014896000500848, (unknown phone number),

IMEI: 014896000500848

7) LG, Mod. M257LG, SN: 801CYEA357652, 918-442-5855,

IMEI: 35575083576522

The devices are currently located at 333 W. 4<sup>th</sup> Street, Suite 3820, Tulsa, Oklahoma, 74103, under PACTS ID: 6692.

The warrant authorizes the forensic examination of the devices for the purpose of identifying the electronically-stored information described in Attachment B.

**ATTACHMENT B**

1. All records on the Device described in Attachment A that relate to the unlawful drug distribution in violation of Title 21, United States Code, Sections 841, 844, and 846

- a. records relating to communication with others as to the criminal offenses above; including incoming and outgoing voice messages; text messages; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
  - b. records relating to documentation or memorialization of the criminal offenses above, including voice memos, photographs, videos, and other audio and video media, and all ExIF information and metadata attached thereto including device information, geotagging information, and information of the relevant dates related to the media;
  - c. records relating to the planning and execution of the criminal offenses above, including Internet activity, including firewall logs, caches, browser history, and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;
  - d. application data relating to the criminal offenses above;
  - e. lists of customers and related identifying information;
  - f. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
  - g. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
  - f. all bank records, checks, credit card bills, account information, and other financial records.
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. All records and information related the geolocation of the Device at a specific point in time;
4. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the statutes listed in Paragraph 1 of this Attachment.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT C

